Network vs. Host-Based Vulnerability Management

A Spire Research Report – July 2004

By Pete Lindstrom, Research Director

Spire Security, LLC
P.O. Box 152
Malvern, PA 19355
www.spiresecurity.com

Executive Summary

Vulnerabilities are the weaknesses in the computing fabric of an enterprise that must be assessed and acted upon in order to reduce the risk of compromise. While most security professionals understand this, the approaches to managing vulnerabilities through remediation, mitigation, and elimination are varied and confusing. In particular, two of the primary approaches involve either a network or host-based vulnerability management solution.

This white paper provides a basic framework for vulnerability management in an enterprise. More importantly, it identifies two solutions that are often confused – network vulnerability scanners and host-based vulnerability scanners – and defines the strengths and weaknesses of the two in comparison to each other.

Finally, the paper discusses Symantec's Enterprise Security Manager, a host-based vulnerability assessment solution, and its value proposition to the enterprise.

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues. Spire provides clarity and practical security advice based on its "Four Disciplines of Security Management," a security reference model that incorporates and relates the functions of identity management, trust management, threat management, and vulnerability management. Spire's objective is to help refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was commissioned by Symantec Corporation. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.

Network vs. Host-Based Vulnerability Management

Table of Contents

Introduction

In information security, a vulnerability is generally associated with a specific, known weakness in a software program. Sometimes, these vulnerabilities exist as software flaws or "bugs" in software where the weakness is due to improper programming during development. Other times, the vulnerability occurs as a configuration weakness, such as a user account without a password. In either of these scenarios, a system may be compromised in some way.

In addition to vulnerabilities that lead to direct compromise of a system, there also exists weaknesses in configurations that may indirectly lead to compromise by providing key information about directory structures, command usage, or system attributes. MITRE's Common Vulnerabilities and Exposures (CVE) project directly references this situation by delineating the difference between a "universal vulnerability" and an "exposure" (see http://cve.mitre.org/about/terminology.html for details).

This latter group of exposures is the subject of great debate in information security, particularly when evaluating "out of the box" security or hardening systems through configuration. Exposures have a functional purpose to go along with the weakness, and therefore some cost/benefit analysis and risk assessment must be done to determine whether it should be allowed in an environment. Enterprises often do this when constructing policy documents that reflect technical standards and configurations of systems.

Though vulnerability assessments are often thought of as reactive activities in search of unpatched systems, in a broader sense they include policy compliance reviews that check for the presence of controls as defined by corporate business objectives.

Ultimately, a security professional should be aware of known vulnerabilities as well as exposures to his or her environment – it is the only proper way to conduct a risk assessment. The practice of vulnerability management involves identifying all of these weaknesses so that proper controls and defenses can be put in place to protect them.

Vulnerability Management Lifecycle

Vulnerability management involves identifying and evaluating the impact of vulnerabilities and exposures in an environment and providing a controlled process to address them in some way. An effective vulnerability management program incorporates information about the enterprise computing environment that is refreshed and continuous. The initial steps include:

- **Inventory** the environment to determine what systems exist and what services and applications are running.
- **Assign** responsibilities for data ownership, system administration, and security management.

- **Develop** policies, procedures or technical guidelines that define key characteristics and attributes of the systems.
- **Plan** the process for ranking and addressing vulnerabilities as they are identified.

This information collection and process development is an ongoing activity that supports the key vulnerability lifecycle that includes identifying new vulnerabilities, scanning for the vulnerabilities, evaluating the results, determining a course of action, and reviewing progress – identify, scan, evaluate, act, review.

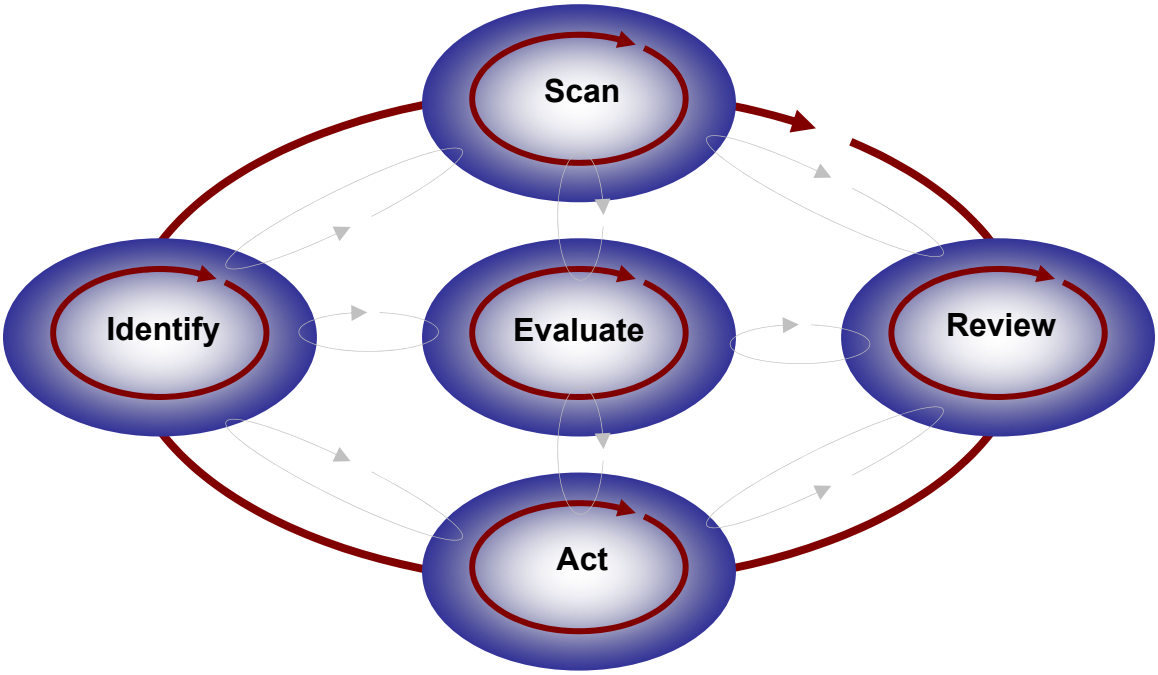

Table 1. Graphic depiction of the five step vulnerability management process.

Step 1 - Identify and Define New Vulnerabilities

The first step in the lifecycle is to identify new vulnerabilities through research and other sources of information, then define a method to identify these vulnerabilities on the systems being scanned. Usually, this step begins with the vendor or consultant reviewing announcements, evaluating software code, and testing systems to validate vulnerability claims. Sometimes enterprises may create their own custom network scans or search a configuration database to identify the specific attributes that are affected.

When a new vulnerability is identified, an impact assessment must be done to determine the level of damage that can be done. Typical considerations for this initial impact assessment (which will be revisited during the prioritization phase) are the nature and type of systems at risk, the value of the assets on those systems, and the extent of the damage that may occur - whether an exploit of the vulnerability may result in full system control, denial-of-service, enumerated information, or some other effect.

Step 2 - Scan the Computing Environment

The scan is the primary step in identifying specific vulnerabilities within an organization's computing environment. In general, scans are performed in two ways – the periodic scan or the targeted scan.

The periodic scan identifies all known vulnerabilities and policy deviations associated with a particular platform by performing routine scans periodically – usually once a quarter, month, or week. These scans are agnostic to impending threats and generally provide an ongoing proactive means for securing the environment. The periodic scan is the typical technique for auditors and policy managers to evaluate the effectiveness of controls and compliance with policy.

The second type of scan is the targeted scan. The targeted scan looks for signs of a specific vulnerability – usually a recently identified one – across the entire computing environment. The targeted scan is run when necessary and is normally used to identify the extent of any particular weakness in an environment. The targeted scan is often used in conjunction with patch management exercises to determine which systems need to be patched.

A scan identifies specific attributes of objects, such as the patch level of an operating system, a registry setting, or an unidentified service running on a significant port. There are many elements and objects in a computing environment that provide valuable information in the vulnerability assessment process, including:

- Network-related attributes like services running, protocols in use, and listening ports.
- Operating system information like patch level, system settings, file settings, user account attributes, and registry entries.
- Similar configuration information for Web servers, application servers, and database servers.
- Specific application details from ERP systems (SAP, Oracle Financials, and Peoplesoft) or other enterprise applications from the likes of Documentum, Siebel, and other corporate adopted applications.
- Network devices like routers and switches, wireless access points, firewalls, and networked printers.

The information gathered and methods used are key determinants of success in identifying legitimate vulnerabilities instead of "false positives" and validating noncompliance.

Step 3 - Evaluate Scan Results

When the scan is completed, the real work begins. The results must be evaluated and prioritized. Priority may be assigned based on the nature of the vulnerability, for example a high-risk vulnerability with identified exploit code in the wild, or the value of the system to the business. High-value systems providing significant business functions or hosting sensitive data get higher priority.

Many constituencies – native software vendors, security solution vendors, professional organizations, and others - provide more specific frameworks for prioritizing vulnerabilities. The enterprise may evaluate these and select a "comfortable fit" or keep in mind the general notion of risk being a function of threats, vulnerabilities, and asset value (or incident costs).

Once the identified vulnerabilities are prioritized, they are assigned to responsible parties to take protective action.

Step 4 - Take Action

While vulnerability assessment scans provide good insight into the exposure level of an environment, at some point action must be taken to reduce that exposure and its corresponding risk. There are four options available to address a vulnerability – remediate it, eliminate it, mitigate it, or accept it.

- Remediate - Remediation is the most common response to an identified vulnerability. It involves fixing the specific problem by patching systems with new software updates, changing configuration options to refine the security associated with it and/or upgrading to newer versions.
- Eliminate – Elimination action may be taken by turning off services. It is generally the safest response but potentially the most costly from a business productivity perspective. Presumably, an enterprise has already gone through an elimination process when configuring systems, so existing services are necessary for proper operations. In the case of system or software upgrades, elimination requires much more planning.
- Mitigate – Mitigation is extremely common as both a way to contain certain types of activity within network boundaries (e.g. through a firewall rule) and also a stopgap measure to address new vulnerabilities that are disclosed (e.g. in antivirus and intrusion detection systems). Mitigation involves planning ways to reduce the risk, normally through control and identification mechanisms, without actually eliminating it.
- Accept – It is unreasonable and too costly to eliminate ALL risk. Fixing some vulnerabilities may require critical business systems to be crippled or disabled. If the above three options do not align with business objectives, then simply accepting the risk may be the desired action. This is often referred to as an exception or waiver.

These alternatives are "mixed and matched" to come up with an effective strategy of risk management.

Step 5 - Review

When some action is taken, it is prudent to verify that it works as designed. This initial review process includes verifying that patches have been applied, testing new configurations, and looking for leaks in network mitigation strategies.

In addition, any change to the environment requires an update to existing knowledgebases and management systems for the computing infrastructure. Constant review involves ensuring that those configuration management databases are up-to-date.

Vulnerability Management Solutions

The flagship product set for any vulnerability management program is the scanner that seeks out the vulnerabilities and controls the assignment of duties and activities, then tracks progress over time. Scanners come in two primary flavors – the network scanner and the host-based scanner. Each is described below.

Network Scanners

The network scanner arose out of the requirements for ubiquitous connectivity that also increase the risk of attack from many different sources. The scanner provides insight into the environment from the network perspective, often taking a "hacker's eye" view of the environment.

Uses

Network scanners are useful for discovering network resources and mapping the ports and services running to various areas on the network. This process helps build the "universe" of systems that an organization has and its corresponding exposure.

In general, network scanners discover network resources, look for open ports on the network, identify and classify the service running, and then test the service to identify attributes like patch levels. Scanners also can emulate protocol activity at lower layers to test how a system responds to these communications.

What it Measures

Network scanners evaluate network security for the accessible areas of the network. Given that the scanner is network based, its position on the network drives its visibility into the services running throughout the environment. Scanners are especially useful at identifying points of entry and attack into a network, since they follow the path of the hacker. These points of entry may be characterized as the "apparent risk" of an enterprise – the risk that manifests itself in outward-facing exploitable services.

Penetration Testing

Network scanners can sometimes extend their reach by not only identifying apparent vulnerabilities, but by attacking them in a controlled manner. In this way, an enterprise may be able to test the likelihood of exploit without suffering from a real attack. Penetration testers provide some automatic and manual control over attacks and generally keep track of all activity to provide a complete record of what types of attacks were attempted.

Host-based Assessment

The host-based vulnerability assessment (VA) solution arose from the auditors' need to periodically review systems. Arising prior to the Internet becoming popular, these tools often take an "administrator's eye" view of the environment by evaluating all of the information that an administrator has at his or her disposal.

Uses

Host VA tools look at system configurations, user directories, file systems, registry settings, and all sorts of other information on a host to gain knowledge about it. Then, it evaluates the possibility of compromise. It may also measure compliance to a predefined corporate policy in order to satisfy an annual audit. With administrator access, the scans are less likely to disrupt normal operations since the software has the access it needs to see into the full configuration of the system.

What it Measures

Host VA tools can examine the native configuration tables and registries to identify not only apparent vulnerabilities, but also "dormant" vulnerabilities – those weak or misconfigured systems and settings that may be exploited after an initial entry into the environment.

Host VA solutions can evaluate the security settings of a user account table; the access control lists associated with sensitive files or data; and specific levels of trust applied to other systems. The host VA solution can more accurately determine the extent of the risk by determining how far any particular exploit may be able to get.

Comparing Network and Host Assessment Solutions

Network Scanners

Network scanners provide the "hacker's eye" view of the network and its exposure.

Network scanners are quicker and easier to deploy. These solutions can operate from anywhere, anytime, so they can be made almost immediately useful. Network scanners are generally configured to scan IP address ranges, so they are good at picking up rogue devices on the network, strange services being run, and other network-related activity.

The success of a network scanner, however, must be tempered with an understanding that its strength (being network-based) is also a limiting factor. Network scanners may not have deep access into host systems, either because they are operating at a lower level of privilege or because they are scanning from an area on the network that doesn't have full access to all systems. In general, the more security hardened a system is, the less information a network scanner is able to obtain.

Host-based Scanners

Host-based vulnerability assessment solutions provide the "administrator's eye" view of the computing environment and its exposure.

Host-based vulnerability assessment tools can provide insight into the potential damage that can be done by insiders and outsiders, once some level of access is granted or taken on a system. They are generally useful in identifying weaknesses behind an initial control setting.

Host-based tools are generally more difficult to deploy than a network scanner, sometimes requiring agents installed on systems. This is self-limiting and inhibits the discovery of new or rogue systems within the computing environment.

The chart that follows compares and contrasts the differences between the network approach and the host-based approach to vulnerability assessment.

Network Scanner	Host-based Scanner
Provides a "hacker's" eye view of the computing environment by identifying network-facing apparent vulnerabilities.	Provides an "administrator's" eye view of the computing environment by identifying system configuration attributes and settings.
Less time-consuming to deploy – only requires network access.	More time-consuming to deploy – requires system access and may use agents deployed on hosts.
Less time-consuming to upgrade software.	More time-consuming to upgrade software (where agents are required).
Usually needs regular updates to identify new vulnerabilities.	Needs regular patch updates, but is also user-configurable to identify new vulnerabilities.
Scans full range of IP addresses and identifies rogue or unknown network resources.	Scans system configurations and identifies latent vulnerabilities (non-network facing) and exposures.
More intrusive scans based on testing requirements to minimize false positives.	Less intrusive scans with full system access and fewer false positives.
More bandwidth intensive and time-consuming scans.	Less bandwidth intensive and less time-consuming scans.
Collects snapshot information based on the time of the scan. (Assumes always-on connections).	Can push out updated information when a system is powered on or connected to the network.
Infrastructure-dependent based on location of scanner versus resources being interrogated.	Infrastructure independent with full system access to identified systems.
Evaluate network-oriented policies such as service and protocol usage.	Evaluate system-configuration policies such as running services, user account configurations and access control rights.
Often don't require the input and feedback of multiple constituencies within an organization to deploy.	Host agents may be more difficult to deploy, often requiring the input and feedback of multiple constituencies within an organization to deploy.

Chart 1: Capabilities comparison between network scanners and host-based scanners for vulnerability assessment.

Symantec's Enterprise Security Manager

Symantec Enterprise Security Manager™ (ESM) is a host-based vulnerability assessment solution that rigorously evaluates over 35 different operating systems, and numerous databases, and Web servers baseline security policies to ensure they are configured and patched properly. In addition, ESM also finds and reports on known vulnerabilities that could be maliciously exploited. ESM gives companies a way to ensure their systems are compliant with stringent usage standards and that vulnerabilities are discovered and promptly fixed.

Configuration and Deployment

Symantec's ESM uses a three-tier manager-agent-console architecture to manage up to 10,000 systems per ESM Management Console and 2,000 agents per ESM Manager. The systems can be configured to support centralized or distributed hierarchies with included separation of duties capabilities. ESM can be configured to automatically run its scans (audits or policy runs) and automatically update its software and patch content at scheduled times.

Security Awareness and Risk Assessment Capability

ESM automatically assesses critical business delivery systems (servers, applications, networks and security controls) for violation of policy and discovery of missing patches required to eliminate exploitable vulnerabilities. This allows companies to better understand their security and risk posture and to better plan and prioritize future security spending.

Support for Industry Standards and Regulations

ESM provides templates that support compliance reporting capabilities. These modules provide detailed reporting for standards like ISO 17799, FISMA, NERC security standards, and Visa's CISP as well as regulations like HIPAA, Sarbanes-Oxley, and Gramm-Leach Bliley. ESM's policy capabilities extend to Oracle, DB2 and Microsoft SQL Server databases and IIS, Apache and iPlanet Web servers. Each policy check is backed by Symantec research that maps the checks to sections in the respective policy documents.

Symantec Security Research

Enterprise Security Manager receives regular updates of best-practice policies and assessment capabilities that allow it to discover newly discovered vulnerabilities and configuration violations in operating systems, databases and applications. Symantec has created a security research organization, Symantec Security Response, that identifies emerging threats globally and provides regular and timely updates for managing emerging security threats.

Holistic Risk Mitigation

Often times organizations have a difficult time prioritizing all security issues / risks. ESM reports security policy violations to Symantec Incident Manager (IM) to be correlated with IDS, firewall, and antivirus (AV) events to properly characterize holistic, meaningful security incidents. These incidents are prioritized in IM guiding the organization into addressing the most important security issues with its limited resources.

Spire ViewPoint

Vulnerability management is one of Spire Security's core Four Disciplines of Security Management. It is the activity that provides the most control and best way to secure the enterprise – through basic hardening of systems and management of their configurations. When evaluating solutions in the vulnerability management space, it is important to understand the nature and extent of any solution to determine whether it provides full coverage over the computing environment.

The host-based vulnerability assessment solution has history on its side. It arose in the days of proprietary systems to gain knowledge about system configurations. These solutions evaluated weaknesses prior to the Internet, when attackers were exploiting weak controls to gain access to data.

Network-based solutions arose with the onset of the TCP/IP networking standard and the Internet, to identify network-accessible vulnerabilities and to regiment penetration testing into a repeatable process that tested the network infrastructure rather than the pentester's abilities.

Both network and host-based approaches provide differing value propositions to an organization. Network-based solutions are especially useful for quick deployments to assess the network-facing risks. They can be up and running within minutes in some cases and don't require the input and feedback of multiple constituencies within an organization to deploy. Host-based solutions are better at identifying configuration and policy issues associated with more in-depth operating system, database, and application programs. Host-based solutions are more accurate, will generally provide more insight into configurations and collect more knowledge about each individual platform in order to properly assess the corresponding risk.

A combination of host and network VA is the most complete and desirable solution. At a minimum, host-based VA should be deployed to mission-critical servers. Network assessments should be used to determine the strength of the host-based VA controls being checked as well as assess other networked devices that do not/cannot have host VA agents installed.

Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper was commissioned by Symantec Corporation. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.